SMART GRID INTEROPERABILITY PANEL

Smart Grid Testing & Certification Committee (SGTCC)

Interoperability Process Reference Manual (IPRM)

Version 2.0

FINAL DRAFT – December 15, 2011

Interoperability Process Reference Manual (IPRM)

RIGHT TO DISTRIBUTE AND CREDIT NOTICE

DISCLAIMER

This document is a work product of the Smart Grid Interoperability Panel. It was prepared by the participants of the SGIP and approved by the Smart Grid Interoperability Panel's Plenary Leadership. Neither the National Institute of Standards and Technology (NIST), the SGIP leadership, its members nor any person acting on behalf of any of the above:

- *MAKES ANY WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, with respect to the accuracy, completeness, or usefulness of the information contained in this report, or that the use of any information, apparatus, process, or composition disclosed in this report may not infringe privately owned rights; or*
- *Assumes any liabilities with respect to the use of, or for damages resulting from the use of, any information, apparatus, process, or composition disclosed in this report.*
- *Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the Smart Grid Interoperability Panel.*

THIS IS NOT A NIST DOCUMENT

Interoperability Process Reference Manual (IPRM)

THE SGIP

The Smart Grid Interoperability Panel (SGIP) is a membership-based organization established by NIST and administered by a NIST contractor to provide an open process for stakeholders to participate in providing input and cooperating with NIST in the ongoing coordination, acceleration and harmonization of standards development for the Smart Grid. The SGIP also reviews use cases, identifies requirements and architectural reference models, coordinates and accelerates Smart Grid testing and certification, and proposes action plans for achieving these goals. The SGIP does not write standards, but serves as a forum to coordinate the development of standards and specifications by many standards setting organizations.

Contents

Interoperability Process Reference Manual (IPRM)

Preface

About the SGTCC

The Smart Grid Testing & Certification Committee (SGTCC) is a standing committee within the Smart Grid Interoperability Panel (SGIP), the organization initiated by the National Institute of Standards and Technology (NIST) to coordinate standards deployment for the Smart Grid. The SGTCC mission is the creation of

- organizational frameworks,
- methodologies, and
- documentation

relating to compliance testing and product certification on Smart Grid interoperability and cybersecurity based standards.

The SGTCC is composed of a broad range of volunteers with expertise in testing and product certification associated with utilities, vendors, independent test labs, accreditation bodies, associations and consortia that operate certification programs, standards bodies, and government. The SGTCC is open to all interested individuals with testing and certification expertise and responsibility, with leadership provided by an SGIP-elected panel of approximately 30 voting participants.

Contact the SGTCC

Questions or comments about this document, as well as general inquiries about the SGTCC may be directed to:

Rik Drummond, SGTCC Chairman (rikd@drummondgroup.com)

or

Rudi Schubert, SGTCC Program Administrator (rschubert@enernex.com)

1. IPRM Executive Summary

The SGTCC has developed and issued this Interoperability Process Reference Manual (IPRM) detailing its recommendations on processes and best practices that enhance the introduction of interoperable products in the market place. These recommendations build upon international standards based processes for interoperability testing and certification.

Implementation of the IPRM by Interoperability Testing and Certification Authorities (ITCAs) will increase the quality of standards-based, secure and interoperable products in the Smart Grid marketplace.

The SGTCC believes that implementation of the IPRM will lead to reduced deployment costs of Smart Grid systems and devices, and enhanced product quality with respect to interoperability and conformance, ultimately providing increased end-user customer satisfaction, and confidence to the buyer through meaningful certification programs.

The IPRM is a key foundational element of the SGIP Testing and Certification Framework. It will enable the adoption of consistent and measurable certification and testing policies and procedures across Smart Grid products (utilizing standards) based on the conformance, interoperability, and cybersecurity testing experience and expertise of SGTCC participants, and the widely accepted ISO/IEC 17025 and ISO/IEC Guide 65 international standards for testing laboratory and certification body management systems.

The ISO/IEC testing and certification standards provide a solid foundation for the development and operation of high quality testing and certification programs. The SGTCC also recognized that additional technical requirements and best practices are necessary to help assure test program tech-

nical depth and sufficiency in meeting end user expectations for interoperability and cybersecurity. These additional recommendations are detailed in this IPRM.

1.1. Purpose and Problem Statement

The IPRM is intended to enhance the validity and consistency of testing and certification programs for standards based products in the market place to help assure their conformance and interoperability for the end user/buyer.

The SGTCC has identified the need for testing and certification programs with uniform quality processes (ISO 9001, *Quality Management Systems - Requirements* based) across all products based on Smart Grid standards. Additionally there is a need for third party assessment and accreditation services to be available to help assure that these programs achieve the technical and quality expectations of end users.

Trusted 3rd party certification programs require specific and detailed test requirements, pass/fail metrics, and defined processes to enable a consistent and well-understood approach to testing, and the subsequent assessment of the test certified results. There can be little left to interpretation as a vague or undefined process will lead to inconsistent application and conclusions providing negligible benefit to end users.

3rd party, independent and trusted certification programs associated with some of the Smart Grid standards under consideration for the SGIP Catalogue of Standards do exist, however there is significant variability across those programs with respect to the depth of testing and the detailed processes, policies and practices in place to support the granting of certification. This presents an additional dimension to the problem as there is a need for all Smart Grid certification programs to be meaningful and rigorous to increase end user confidence in their product decisions related to interoperability between products and systems.

The IPRM seeks to address these issues described above and provide the recommendations of the SGTCC in structuring robust testing and certification programs, and the means to assess the success of ITCAs in their implementation of the IPRM recommendations.

1.2. Present Testing Flow

The diagram below illustrates a basic testing approach presently used for Smart Grid systems and devices.

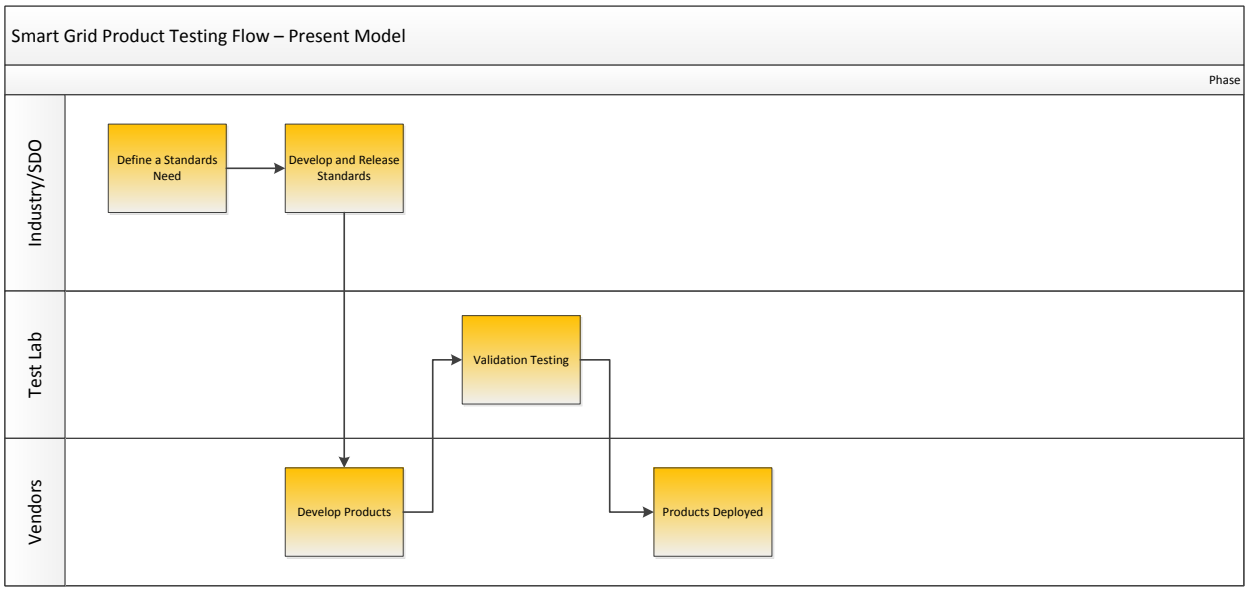

Figure 1 – Smart Grid Product Testing Flow – Present Model

In this model, standards are developed by industry and vendors use these standards for their product design and testing. Testing may be done internal to the vendor, onsite at a utility or other end user laboratory, or working with an independent provider of testing services.

This model is straight forward and useful; however in the absence of a broader framework, there are broad variants in the approach and depth of testing programs, leading to uncertainty in whether or not the testing is achieving the needs of end users. A number of current industry programs offer options for certification, usually for conformance to a specification. However a majority of programs simply include basic testing and result reporting, and do not go so far as to certify conformance or especially interoperability. Thus the end buyer is not assured of conformance and interoperability quality products in the market place.

1.3. Future Testing Flow

The diagram below illustrates one possible future testing model proposed by the SGTCC for Smart Grid systems and devices. It goes beyond the various basic programs currently available introducing a new concept of ITCAs as test and certification program owners responsible for implementing a consistent high quality framework across test programs within their scope of operations. Additionally, accreditation bodies are introduced to independently validate that ITCA certification bodies and test labs are indeed adhering to the recommended practices. This will provide greater confidence to end users in products that exhibit interoperability and conformance. It should be noted that this specific testing model may not be applicable for all situations; however the core concepts are recommended by the SGTCC where practical for implementation.

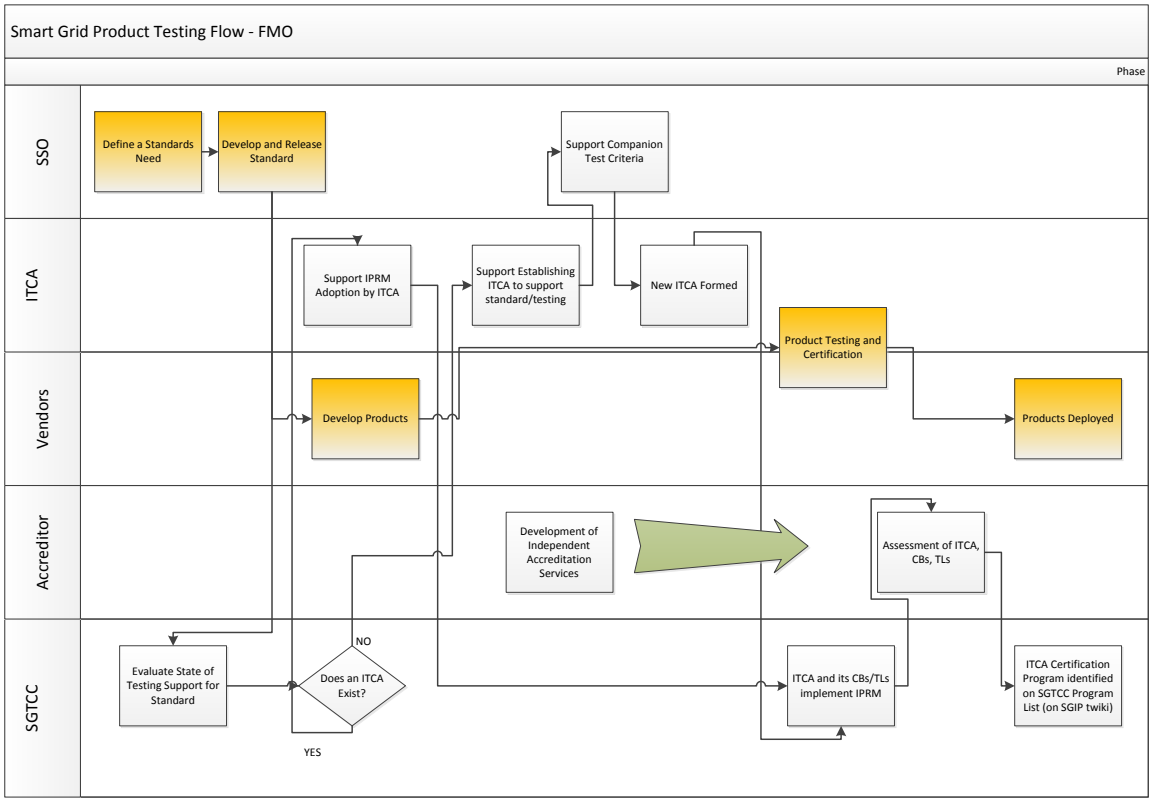

Figure 2 – Smart Grid Product Testing Flow – Future Model

1.4. Intended Audience

The IPRM is the center of the SGIP's testing and certification framework, and as such affects a broad range of stakeholders. The IPRM most directly affects and is operationalized by:

- Interoperability Testing and Certification Authorities (ITCAs),
- Certification Bodies (ISO/IEC Guide 65),
- Test Laboratories (ISO/IEC 17025) and
- Accreditation bodies.

System and device vendors are also key stakeholders both in how the IPRM affects their products under test, and their internal test laboratory operations. End users and buyers are the customers and should be able to expect interoperable products in the market place. In addition, the value of IPRM implementation is enhance where these customer understand the standards and associated certifications, and include specific interoperability and certification requirements in RFPs.

The IPRM defines the responsibilities within and among the ITCA, SSO (Standards Setting Organizations), accreditors, test lab(s) and the certification body designed to bring interoperable standards based products to market. The IPRM implementation is facilitated through the use of check lists to ensure key areas are addressed. It is also important that ITCAs communicate well with end users in conveying the value of the certifications that they provide and how they may be used in assessing and achieving product interoperability.

These responsibilities require detailed processes, which are left to the individual ITCA to define. However, the IPRM **REQUIRES** that product certification be issued by an ISO/IEC 65 accredited third party independent of the testing organization. This follows the logic promulgated in the two basic international management guidelines used as a foundation for the Framework: ISO/IEC 17025, *General Requirements for the Competence of Testing and Calibration Laboratories,* and ISO/IEC Guide 65, *General Requirements for Bodies Operating Product Certification Systems.*

2. International Guidelines for Testing and Certification

The SGTCC extensively investigated and discussed the critical operational processes that independent certification bodies and laboratories need to implement to instill end user confidence in interoperable products. It was quickly concluded that international standards, particularly ISO/IEC Guide 65, General Requirements for Bodies Operating Product Certification Systems[1], and ISO/IEC 17025, General Requirements for the Competence of Testing and Calibration Laboratories[2], were so broadly used and supported, that adoption of these standards for Smart Grid interoperability was a more prudent approach than developing customized criteria that would simply parallel these accepted standards. Further, there is already a system of accrediting organizations and processes in place that support accreditations of testing and certification functions based on these international standards.

2.1. Overview of ISO/IEC 17025

ISO/IEC 17025 is focused on test laboratories and contains requirements that labs need to demonstrate that they operate a quality management system, are technically competent, and are able to generate technically valid results. It incorporates all requirements of ISO 9001, Quality Management Systems – Requirements, that are relevant to testing services and facilitates acceptance of test results from accredited laboratories. Accreditation bodies apply these requirements in their laboratory assessments.

[1] http://www.iso.org/iso/catalogue_detail.htm?csnumber=26796

[2] http://www.iso.org/iso/search.htm?qt=iso+17025&searchSubmit=Search&sort=rel&type=simple&published=on

ISO/IEC 17025 can be applied to any testing lab operation, whether independent (i.e. third-party) laboratories or in-house laboratories operated by manufacturers for their own internal product testing. The advantage of applying ISO/IEC 17025 for Smart Grid testing operations is that many labs have already pursued and achieved compliance for selected aspects of the services they offer, and can simply expand their scope of accreditation to encompass new services necessary to support Smart Grid interoperability. This approach will build on common best practices used across the testing industry, speeding implementation and avoiding unnecessary creation of redundant processes.

ISO/IEC 17025 focuses on two major areas of laboratory operations:

1) Management requirements and
2) Technical requirements.

The management requirements address issues such as a lab's documented practices (i.e. both administrative and technical), impartiality of the lab in its operations, responsibilities for continuous improvement and issues resolution, and the active support and involvement of lab management in assuring commitment to complying with these criteria.

The technical requirements focus on areas such as ensuring that lab staff are competent in performing their testing duties, assuring that the lab environment is adequate for services performed, assuring that test plans and other necessary operating instructions are documented and available, and that necessary equipment and software used for testing is calibrated, maintained and appropriate for its intended usage.

The criteria described in ISO/IEC 17025 are extensive and the brief description above simply provides a high level view of some of the key elements that labs need to address in attaining accreditation.

The technical scope of accreditation is specific to the selected tests / services for which the lab applies for evaluation. Evaluations for compliance can be performed by a number of different accrediting bodies, and there are global and regional agreements in place that provide for broad acceptance of an accreditation once attained.

2.2. Overview of ISO/IEC Guide 65

ISO/IEC Guide 65 is for certification bodies and parallels many of the same concepts applied in ISO/IEC 17025 test laboratories. There are general criteria that assure that the organization is non-exclusionary, open and without conflict of interest. Documented administrative policies and processes, as well as documented technical requirements and specifications for certification, are among the required criteria. Criteria are also included to assure that procedures are in place to describe the granting of certifications, as well as ongoing maintenance, extensions and terminations of certifications once granted. Personnel qualifications are addressed for those involved in the evaluation and decision making process associated with the organization's certifications. As in the case for ISO/IEC 17025, this is only a brief description of highlights associated with the more extensive criteria described in the document.

While these international standard guidelines provide a solid foundation for the development and operation of high quality testing and certification programs, the SGTCC also recognized that additional technical requirements and best practices are necessary to help assure test program technical depth and sufficiency in meeting end user expectations for interoperability and cybersecurity. These supplemental criteria are described in subsequent sections of this document.

The IPRM adds an additional REQUIREMENT over and above ISO/IEC Guide 65 -- the independent trusted 3rd party certification authority MUST only allow the statement that products are interoperable only if the products actually demonstrated interoperability during testing. They MUST not assume interoperability from

conformance testing. They MUST demonstrate it before it may be part of the products certification statement.

3. Overview of IPRM Version 2

This section provides an overview of how this Interoperability Process Reference Manual has changed in this latest version and the organization of the document.

3.1. Changes from Version 1

Version 1 of the IPRM was released in January 2011. That version provided extensive background information considered by the SGTCC in the assessment of the state of Smart Grid conformity and interoperability programs, and provided extensive information that would be valuable to readers that may have limited background in testing program models and approaches.

The general goal of this revision was to enhance the utility of the document to support implementation of the criteria and recommendations by an ITCA and to structure it in a way to better facilitate assessments of ITCA implementation both internal to the ITCA and for external independent assessments. The changes in structure and clarity are major. The changes in content are minor.

Fundamentally, Version 2 has an operational focus, while Version 1 provided an informational focus. Most of the key informative material from Version 1 has been retained in this update. The main body of the IPRM emphasizes the operational aspects, while the informational material is provided in a series of separate informational annexes to the document.

Significant changes in IPRM Version 2 as compared to the prior version include:

- Removal of informational/background material --- these removed sections have been transitioned to a new background document that the SGTCC is preparing for release during the first half of 2012

- Greater emphasis on the importance of independent accreditation and adherence to internationally recognized standards for testing labs and certification bodies
- Restructuring the document sections to align with the interests of key stakeholder groups – ITCAs, Cybersecurity testing organizations, certification bodies and test laboratories – the revised sections are targeted at the interests and responsibilities of specific stakeholders
- An expanded section on cybersecurity – this topic was covered briefly in IPRM V1 and provided much more detailed coverage in this new release
- The requirements tables in Version 1 were reviewed and condensed to eliminate redundancy and non-measurable criteria. The tables were also relocated in the document to align with the applicable sections (removes the need to jump back and forth between sections of interest). The requirements in IPRM V2 are intended to be more easily implementable for third party accreditation and other assessment operations.

3.2. Organization of the IPRM

The preceding sections provide the necessary background to understand the issues addressed by the IPRM, the SGTCC philosophy in addressing the issues, the objectives of the IPRM in solving the issue and the basic foundation of international standards upon which the IPRM is constructed.

The IPRM considers these international standards (ISO/IEC Guide 65 and ISO/IEC 17025) as fundamental foundation elements to be implemented in Smart Grid interoperability testing and certification programs. The SGTCC has identified other detailed recommendations and requirements that extend beyond the baseline criteria found in the ISO standards. These are addressed in subsequent section of the IPRM as follows:

- Section 4 - ITCAs and their implementation of the IPRM
- Section 5 - Recommendations and requirements for ITCAs beyond those identified in ISO/IEC Guide 65 and ISO/IEC 17025
- Section 6- Recommendations and requirements specific to Cybersecurity Testing
- Section 7 - Detailed Tables of Criteria recommended for implementation by ITCA Certification Bodies and Test Labs

4. ITCA Implementation of the IPRM

The SGTCC strongly advocates the implementation of an Interoperability Testing and Certification Authority (ITCA) organization to support each Smart Grid standard.

The implementation of the IPRM by an ITCA is intended to accomplish several goals:

- Increase the buyer's confidence in the purchase of neutral 3rd party certified interoperable products for their organizations over time
- Standardize the testing and certification processes, through a set of best practices, used for all smart grid products
- Provide a basis for an approval process for those organizations following the IPRM to assure the purchasing organizations of quality, audited testing programs. The SGTCC believes that end users purchasing Smart Grid products based on standards will save money and shorten product implementation cycle time by using products that comply with the SGIP TCC Framework.

4.1. What is an ITCA?

An Interoperability Testing and Certification Authority (ITCA) is the program management organization, providing oversight for testing and certification activities associated with one or more standards or specifications, that takes responsibility to insure that interoperable products within the scope of the specific ITCA program are brought to market. The ITCA coordinates the participation of certification bodies and test labs for its program.

An early finding of the SGTCC was that standards that had an associated ITCA engaged in test and certification of products to the standard were more rapidly implemented and adopted by the market place.

The SGTCC has established the following required practices for ITCAs, certification bodies and test laboratories:

- Certification bodies (CBs) should be accredited to ISO Guide 65, *General Requirements for Bodies Operating Product Certification Systems*
- Test laboratories should be accredited to ISO 17025, *General Requirements for the Competence of Testing and Calibration Laboratories*
- The ITCA should have an agreement with an accrediting organization(s) to assure that Certification Body and Test Lab accreditation is being performed in accordance with the ITCA program scheme.
- An ITCA should have a strong relationship with the SSO associated with the standard for the purpose of feedback towards standard improvement and clarification where there may be ambiguities

The requirements for adherence of ITCAs to these internationally recognized industry standards is consistent with the practices exhibited in other industry programs engaged in testing and certification activities related to critical infrastructure (e.g. FCC programs for communications networks) and issues impacting personal safety and security (e.g. OSHA NRTL safety programs).

4.2. How does an ITCA implement the IPRM?

An ITCA begins its implementation of the IPRM by declaring their intent to participate in the program and implement the IPRM recommendations in their program scheme. This step is formalized by completion of the ITCA Application Form located on the SGTCC Twiki site:

http://collaborate.nist.gov/twikisggrid/bin/view/SmartGrid/SGTCCIPRMImplementation

Submittal of the ITCA Application Form indicates that the ITCA has entered a transitional phase during which time they are actively engaged in integrating the IPRM recommendations in their program. The SGTCC recognizes that implementation is a significant investment for the ITCA. The SGTCC will recognize those ITCAs that have committed to the IPRM by acknowledging their participation on the SGTCC TWiki site.

As an acknowledged participant in IPRM implementation, the ITCA must be able to clearly demonstrate that they are progressing with their implementation activities in a timely manner. The SGTCC retains the right to remove its ITCA program acknowledgement where it concludes that the ITCA is not actively implementing the IPRM and/or fulfilling other obligations necessary to achieve IPRM implementation.

In the longer term, it is expected that an ITCA will fully implement the IPRM recommendations, utilizing certification bodies that have been independently accredited to ISO Guide 65 and test laboratories that have been independently accredited to ISO 17025. At the time of release of this document, the SGTCC is actively engaged in dialogue with accreditation organizations to facilitate the availability of these assessment services in 2012, with the key IPRM recommendations integrated into the independent accreditation criteria.

477

478 4.3. Relationship between Accreditation Bodies, ITCAs, 479 Certification Bodies and Test Labs

480

481 The diagram below depicts the relationships across the key elements of testing and certification
482 programs in the view of the SGTCC. ITCAs may be structured with subtending certification bodies
483 and test labs dedicated to its mission. Alternatively, the ITCA may serve a dual role, acting itself as
484 the certifying body. The SGTCC recognizes that flexibility is necessary in ITCA structure to ac-
485 commodate the diverse needs across the many technologies that are a part of the Smart Grid.
486 While that flexibility and any necessary innovation are encouraged by the SGTCC, the one con-
487 stant required is the need for checks and balances in the process such that certification decisions
488 are made by personnel independent of those developing test data.

489

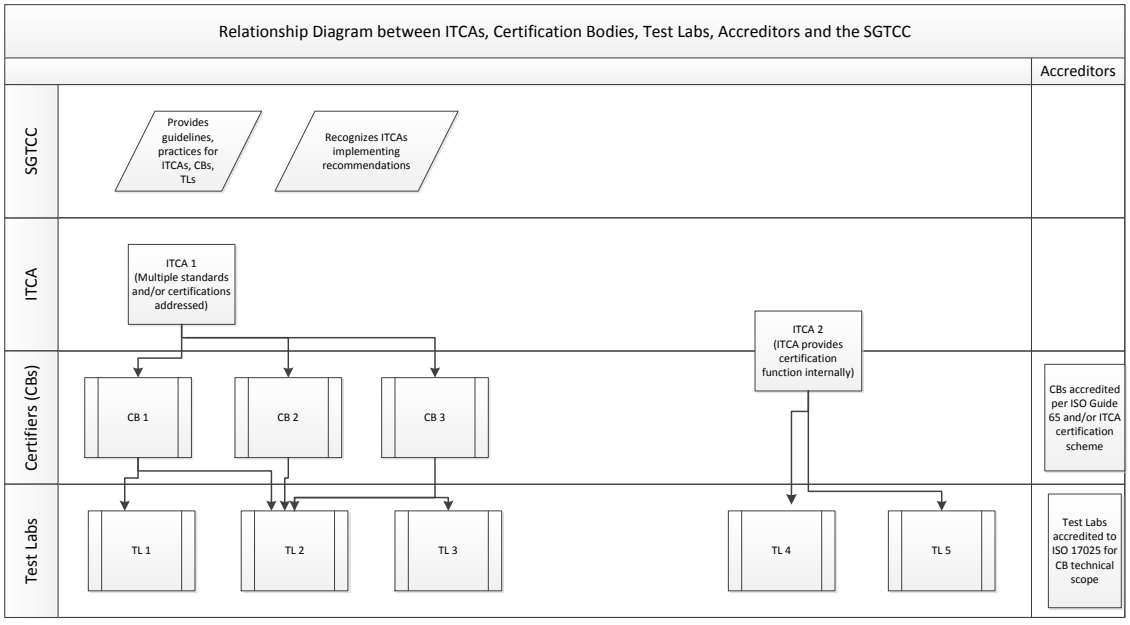

Figure 3 – Relationships between Accreditation Bodies, ITCAs, CBs, TLs, and SGTCC

490

5. Interoperability and Conformance Test Construction

This section provides requirements, best practices and guidelines for ITCAs in their development and operation of interoperability and conformance testing programs. The recommendations provided in this section were generated based on input from experienced testing organizations that have evolved interoperability and conformance programs through lessons-learned in executing tests for both software and hardware applications.

The recommendations may not apply directly to all testing applications; however, they should be considered for interoperability and conformance test programs as these practices have proven to be valuable in executing a broad cross-section of program types.

Each ITCA should evaluate how these recommendations, observations and practices apply to their specific programs, and incorporate the recommendations into their programs where applicable.

An ITCA SHALL manage the end-to-end processes associated with interoperability testing and certification. It is expected that the ITCA has the appropriate infrastructure in place to support this function. Where a new ITCA is being launched in support of a standard, establishment of the following is recommended:

- Business plan
- Clear governance structure and IPR policy
- Testing lab(s)
- Certification body / bodies

The requirements in this section, as well as those provided in Section 6 for Cybersecurity and in Section 7 for Certification Bodies and Test Labs SHALL be implemented by the ITCA in its programs to enable product interoperability, cybersecurity and quality testing and certification services.

5.1. General Test Policies

- ITCAs must provide explicit information on the requirements, processes and expectations associated with their program to prepare vendor participants for the certification process. Example information required includes, but is not limited to, eligibility criteria to establish that the program is appropriate for a specific product, how to prepare for certification, and requirements for specific test environments (i.e. GUI applications to access low-level APIs, test scripts, supported browsers, dedicated test hardware, samples, etc.) in order to conduct testing.
- Final Test Reports should include at a minimum:
    - Organization(s) that conducted the tests and location(s) where the tests took place
    - Test completion dates
    - Product name / version / release tested
    - Type of tests (i.e. interoperability or conformance)
    - Test script version information
    - Standards version information
    - Technique(s) used for a test including standards and procedures followed
    - Test profile used or a list of test cases if a complete test profile is not used
    - Test equipment used, and all equipment traceability statements.
    - Where interoperable results are claimed, details on the extent, conditions and/or limitations in the findings SHALL be fully identified

- If a certification program limits the length of a certification, this information should be communicated so that product providers and end users are aware of any such expiration in validity. Criteria for expiration is an ITCA business decision, and may be based on factors including but not limited to, standards revisions and product changes.
- An interoperability testing program shall determine whether or not interoperability has been demonstrated between all products within the scope of the test. The ITCA must not assume conformance testing achieves interoperability unless significant market based historical evidence that their tested products are completely interoperable using conformance based methods. Additionally, such evidence should be thoroughly and formally recorded, for example as collected for ISO Guide 65 surveillance activities – anecdotal information or lack of reported interoperability problems is insufficient. The ITCA or certification body must not declare they have achieved interoperability in the products unless one or both of the above conditions (test reports/data or documented market based evidence) is qualitatively achieved and demonstrated.
- A certified interoperable product SHALL be conformant to the standard unless full conformance causes interoperability issues. In such cases, the issue should be reported back to and formally recognized by the ITCA and/or the SSO so corrective action can be taken.
- The level of Interoperability and Conformance testing is always a trade-off between cost and test coverage. It is highly recommended that the ITCA perform a cost-benefit analysis on the degree of coverage associated with the test for both conformance and interoperability against the cost to test. In determining the test coverage, the security and safety concerns along with appropriate NERC / similar requirements should be considered paramount in determining the coverage assessment.
- Proper test tools produce reliable, repeatable and traceable test results. Such tools require validation processes, test suites, tool documentation, test reports, calibration certificates and other relevant artifacts. The validation of the test tools must be performed against a

571 defined sample of software and / or hardware implementations under test. Refer to ISO /
572 IEC 17025 for more detail on the use of qualified and calibrated test tools[3].
573

574 ## 5.2. Test Suite Specification (TSS)
575
576 A TSS consists of a suite of tests, categorized into logical functional areas, such as use cases or
577 well-defined features. Each test suite consists of many related test cases corresponding to a par-
578 ticular feature set or use case. A test profile evaluates a subset of a TSS and are used to target
579 specific areas of product interoperability.
580
581 • A common TSS should be established when one or more test labs are deployed to test the
582 same standard and / or profile. If unique test procedures are required to support a test
583 suite, then they should also be defined.
584 • The TSS should be test tool agnostic.
585 • The TSS should be subject to revision control including revision history, revision number-
586 ing, and a defect / expansion management process. The TSS should clearly identify the
587 test purpose, references, resource requirements, test setup, procedures, observable re-
588 sults and possible problems / lessons learned with the test approach. Observables should
589 clearly identify pass / fail / indeterminate requirements and informational elements.
590 • The TSS should clearly define any conventions that will be required to achieve interopera-
591 bility.
592 • The TSS should restrict cardinality and define the exact attributes and associations re-
593 quired for interoperability.
594 • The TSS should remove or clarify all ambiguities and any areas of the standard that may
595 be interpreted differently between two or more interoperable systems.

[3] Recognize that validation and calibration of test tools is a function of the type of test tool being used. For protocol analyzers or frequency measurements calibration is important and defined. For software applications the validation is against the intent in the specification defining the application behaviors. Calibration as such may not apply

- The TSS should be a standard and managed as such by an ITCA or SSO. The documentation should include scope, date of issue, revision, change control, and methods to feedback implementer's results.
- Where applicable, the TSS should specify an approach to validate data and data structures contained in, or produced by, the test.
- Test cases should have clear mappings to feature-sets, use-cases, and requirements.
- An interoperability testing program SHALL determine whether or not interoperability has been demonstrated between all products within the scope of the test. The TSS MUST ensure all areas of the interoperability and conformance testing are sufficiently defined and documented such that the test can be repeated.
- The TSS MUST define the test data required to execute the test cases. The TSS should define any test stub required to execute messages that will generate negative responses.
- The TSS should identify interoperability issues arising from ambiguities in the standard, and make recommendations to the appropriate SSO for improvements in the specification for the standard to prevent those interoperability issues.

5.3. Attributes of a Test Profile in lieu of complete TSS

- MUST be a subset of the TSS
- Specifies mandatory and optional elements
- Specifies all restrictions
- Cannot add to the standard, but can only restrict the standard
- Define the type of profile (i.e. message, model or implementation) and provide a name for the profile that clearly defines the objective / scope of the profile and the use-cases it is designed to test
- Is a companion standard or is submitted to the SSO for progression as a companion standard

5.4. ITCA Technical Program Design Recommendations

This section is taken from the Technical Requirements tables used in IPRM Version 1.

Tech-x	Technical Program Design
	Requirements Description
Tech-1	The ITCA MUST specify in the TSS those features that are mandatory, and those features that are optional.
Tech-2	The ITCA MUST require and enforce that vendors declare the optional features implemented in a product.
Tech-3	The ITCA should require that implementations of optional features be tested and certified for conformance and inter-operability. Furthermore, the ITCA should define common test cases for optional features to be used by all test labs.
Tech-4	An ITCA MUST define the record handling and retention requirements to be followed by the TL and CB functions, consistent with requirements of ISO 17025 and ISO Guide 65. The ISO standards require a record handling/retention policy – the ITCA should define and implement specific details/durations regarding record handling and retention.
Tech-5	The ITCA SHALL specify the conditions under which it will allow for sub-component (e.g., previously certified hardware modules used in developing final products, previously certified software components with well-defined interfaces and dependencies etc.) inheritance in development of final products. However, it is the ITCAs responsibility to ensure that interoperability is maintained.
Tech-6	The ITCA SHALL maintain a controlled list of compatible sub-components that can be inherited to build final products. This might include specifying compatible feature-sets.

Tech-7	When supporting products composed of sub-components, the ITCA SHALL define the set of additional tests necessary to ensure interoperability (e.g. integration testing, final performance testing, etc.)
Tech-8	The ITCA SHALL implement a Compliant Portion Description (CPD)[4] to be used as a guide for assembling a product based on compatible sub-components.
Tech-9	The ITCA SHALL have an explicit process in place to assess necessity of re-certification against subsequent release versions of a specification, including security.
Tech-10	The ITCA SHALL define the level of re-certification required for subsequent release versions of a specification.
Tech-11	The ITCA SHALL define a mechanism to identify the latest version of a previously certified product or system implementation. This is important in cases where a previously certified product or system has been upgraded to a different version.
Tech-12	The ITCA SHALL have a mechanism to enforce version control rules such that each product certification clearly identifies the SSO document and version to which product is certified.
Tech-13	The testing and certification program SHALL have common well-defined standardized test cases. These test cases should be defined in an open, consensus-driven fashion. These test cases will be used by all test labs approved by the ITCA.
Tech-14	There SHALL be a defined correlation between implementations and required testing, commonly called a Proforma Implementation Conformance Statement (PICS).[5]
Tech-15	The testing and certification program SHALL maintain a current and upcoming list of applicable test cases to be called a Test Case Reference List.
Tech-16	There SHALL be a Test Plan derived from the Test Case Reference List and used by all authorized test labs. Tests SHALL be identified using the test plan.
Tech-17	The testing and certification program SHALL require that a static conformance re-

[4] See Glossary of Terms for definition and further explanation of CPD
[5] PICS can be referred as both Protocol Implementation Conformance Statement and Profile Implementation Conformance Statement. Proforma is being used in this requirement to reference both concepts.

	view[6] take place prior to testing a product. This review is used to determine the applicability of the test program requirements relative to the features and functionality of the product under test to assure the test plan addresses all applicable requirements.
Tech-18	The testing and certification program SHALL implement validated test tools. Golden reference test equipment may be utilized where appropriate.
Tech-19	The TSS SHALL be subject to revision control, including revision history, revision numbering, and a defect and expansion management process. The TSS should clearly identify the test purpose, references, resource requirements, test setup, procedures, observable results and possible problems / lessons learned with the test approach. Observables should clearly identify pass / fail / indeterminate requirements and informational elements.
Tech-20	The testing and certification program SHALL assure that defined product test cases cover application profiles for specific feature sets and functions defined by the specific application profile, and implement interoperability evaluation within that application profile.
Tech-21	Where practicable, the testing and certification program SHALL assure that defined product test cases cover all feature sets and functions.
Tech-22	The testing and certification program SHALL assure that defined product use cases are covered in application profiles. Interoperability testing and evaluation SHALL be implemented within those application profiles.
Tech-23	The testing and certification program SHALL classify common or major market products according to their application profiles, and include them as part of an interoperability evaluation for those specific profiles. The evaluation SHALL make use of test profiles correlated to those specific applications.[7]

[6] See Glossary of Terms for the definition and explanation of a static conformance review.
[7] Interoperability testing is tied to market realities. Hence the testing and certification program needs to have a mechanism to adopt representative market products as an integral part of interoperability testing.

Tech-24	The testing and certification program SHALL ensure that venues are provided for multi-vendor and multi-product communication and interchange evaluations (e.g. "plug fests"). This program may be optional for ITCAs correlated to standards resulting in application interfaces and not a physical product
Tech-25	Prototyping of draft standards or major revisions SHALL be supported via multi-vendor / multi-product testing. The ITCA SHALL solicit for the prototyping of draft standards or major revisions, and organize multi-vendor / multi-product testing. It is recommended that the prototyping take place in the late stages of standards development in order to verify the correctness of the standard, verify the test suites and verify that the anticipated interoperability or conformance testing is debugged.
Tech-26	ITCAs SHALL use reference test tools[8] where appropriate to the technology under test (hardware and/or software) to provide a consistent and replicable approach in generating test results across ITCA test labs. Successful testing programs assure that there is a known reference or constant to which the system is evaluated against the desired metrics to determine conformance.
Tech-27	ITCA program tests that are performed across multiple test facilities SHALL implement processes to assure they are each measuring against a common known reference and achieving repeatable results regardless of location.
Tech-28	The ITCA SHOULD have a process to select a minimum of two distinct reference implementations as golden implementations or golden units. The selection is usually based on the results of the interoperability testing. All other implementations SHOULD be tested against these golden implementations.[9]
Tech-29	The golden implementations or golden units SHOULD be clearly associated with

[8] A number of terms are used in describing reference test tools such as "common test harness", "golden reference test equipment", and "golden reference test products". Generally, these each represent test tools available to a test lab or end user to provide a consistent baseline test either as a standalone implementation or in concert with the many other types of test tools available.

[9] The industry prefers three golden units for product testing, but the minimum number of golden units shall be no less than two golden units.

	each version of the standard. Each golden unit is a snap shot (instantiation) of each version of the standard.
Tech-30	If an ITCA Certification Program involves multiple Smart Grid systems, then the Program Requirements SHALL support end-to-end testing of Smart Grid systems involving multiple product implementations to the fullest extent possible.
Tech-31	An ITCA SHALL involve all relevant parties to define various business logic models for the end-to-end system testing, and make scenarios and test harness systems available for testing.
Tech-32	The testing and certification program SHALL ensure that when functional performance requirements are defined in an application profile, the performance test profile(s) SHALL be designed to implement test cases for evaluating these requirements.
Tech-33	The ITCA SHALL ensure that test tools have a complete mandatory feature-set coverage of a standard. In cases where two or more implementations of optional features are available, the ITCA SHALL incorporate those feature-sets in the test tool.[10]
Tech-34	The ITCA SHALL define procedures and processes to validate the use of test tools and reference implementations
Tech-35	ITCA shall develop criteria for surveillance to be carried out by its certification bodies.

5.5. Program and Field Experience Feedback

Successful achievement of interoperability requires a well-communicated feedback process across multiple stakeholders – the ITCA, its testing and certification bodies, standards bodies, end users and vendors. Such feedback loops are essential in the continuous improvement of test programs and the standards upon which they are based. This feedback provides greatest value when it is

[10] Effective test tools need to be able to test all features and functions of a standard. Some features of a standard may never be supported by certain products; however when a standard is published, the industry is free to implement optional feature set in addition to the mandatory set; lack of testing capability of optional feature sets hinders interoperable feature set introduction. Normally, validated test tools have implementations of all features, including optional ones as a condition for the tool validation.

multi-directional, and the ITCA is ideally positioned to manage this information exchange that can help strengthen the base standards and test programs through lessons learned both in the lab and in the field.

An ITCA test program is based on a standard. The ITCA's development of its test methodology provides the opportunity to identify gaps and other issues requiring clarification that should be communicated to the standards body to improve future releases. Similarly, the experiences and lessons learned by the ITCA testing labs can identify criteria in a standard that may present unforeseen difficulties for products to achieve or items not tightly defined that might lead to interpretive differences – again, communicating to the standards body can lead to future improvements.

Perhaps the most critical feedback to be gathered and communicated comes from the end users and product vendors. They can provide definitive feedback on any field interoperability problems associated with "certified" products, necessitating the ITCA and test labs to revisit their test programs to identify any gaps or opportunities to tighten the testing process to help mitigate these interoperability issues in a lab environment, well before products are deployed. This process may also necessitate the ITCA and its certification body reviewing existing "certified" products to determine if any additional testing and analysis is needed to confidently maintain the designation of being certified.

An ITCA program SHALL include a documented surveillance and continuous feedback process to address these potential issues and enhance the interoperability of deployed products.

6. Cybersecurity Testing

The SGTCC has collaborated with the SGIP's Cybersecurity Working Group (CSWG), particularly the CSWG testing and certification sub-working group that has contributed its expertise in preparing this section of the IPRM. Cybersecurity testing and certification issues and practices are a collaborative effort between the SGTCC and CSWG in supporting ITCAs in their implementation of the IPRM recommendations for cybersecurity testing. ITCAs are responsible for coordinating and overseeing the cybersecurity criteria as applicable to the testing and certification programs that they operate. Security related product or system testing is to be conducted when security related claims have been made. If the product does not contain security features, then security is not tested. Security testing can be conducted by a third party; the ITCA does not have to be an expert in security and functionality testing. If the ITCA does outsource security testing, it is imperative that the functionality testing and security testing is tightly coordinated.

6.1. Introduction

Most product vendors make a claim as to functionality and/or offered cybersecurity controls. Organizations need to have a minimum level of assurance that a product's stated function and cybersecurity claim is valid. Confidence in a product's cybersecurity can be based on an impartial cybersecurity evaluation, which includes an analysis of the product and the testing of the product for conformance to a set of cybersecurity requirements and controls. The use of consistent standardized cybersecurity evaluation criteria and methodologies contributes to the repeatability and objectivity of the results. Cybersecurity testing should be performed in conjunction with interoperability tests. As functionality is developed to enable interoperability, new potential vulnerabilities could be discovered. By ensuring cybersecurity testing is conducted with interoperability tests the following objectives are met:

- Uncover design, implementation and operational flaws that could allow the violation of cybersecurity requirements and controls;
- Determine the adequacy of cybersecurity mechanisms, assurances and other properties to enforce the cybersecurity requirements and controls;
- Assess the degree of consistency between the cybersecurity requirements and controls and their implementation;
- Identify and locate loopholes that can cause loss of important information, function, or allow unauthorized access; and
- Identify the cyber security functionality that could impact the interoperability of components and systems.

6.2. Cybersecurity Concepts

The primary objective of cybersecurity testing is to validate the cybersecurity claims. Testing will determine if the product functions as intended and conforms to a defined set of cybersecurity requirements. At a high level, this means providing confidentiality, integrity (authenticity and non-repudiation), and availability for the information stored on the product and system into which the product is integrated..

6.3. Cybersecurity Testing Environment

A critical part of conducting cybersecurity testing is the environment in which the products are tested. Products should be tested in an environment that closely simulates the intended implementation of the product. Cybersecurity testing should conform to identified environmental standards and specifications. An internal cybersecurity policy should be developed for the product being tested which provides the cybersecurity rules under which an implementation or cybersecurity testing environment must operate. In order to understand the security of an implementation being tested, the rules and assumptions about how the implementation must operate need to be specified in particular for mitigations and controls outside the boundary of the implementation. Environmental conditions, particularly when outside the normal operating conditions of a component or system, could

cause a potential critical cybersecurity breach, so they need to be considered during testing. For example, in some extreme temperatures, humidity and radiations, authentication devices can fail even when these conditions are not maliciously induced.

6.4. Cybersecurity Testing Types and Frameworks

The type of cybersecurity tests conducted on a product will depend on the type of product, its functionality, operating environment, and both functional and non-functional cybersecurity requirements. When intertwined with interoperability testing, cybersecurity specific test methodologies should be documented. The interoperability testing results should remain intact and verified after security fixes are applied to address issues found during cybersecurity testing. Different testing methodologies are used to determine attributes (interoperability, conformance, usability, security, etc.) of an implementation being tested. Multiple types of testing techniques should be used, including manual review, fuzz testing, static analysis, dynamic analysis, and penetration testing.

In general, Smart Grid security testing/assessment approaches can be broken into the following major categories:

- **Security Conformance/Certification Testing** is usually initiated by each vendor, to verify that a vendor product meets an industry established level of security, and tested by independent third-party labs using the same testing procedures that are pass/fail in nature. Results of these tests are often published and used in vendor marketing campaigns.
- **Security Interoperability Testing** measures the interoperability of security components between devices and systems from different vendors.

Security Conformance/Certification Testing and Security Interoperability Testing are categories that would typically be within the purview of an ITCA. The following other major categories of Smart Grid security testing/assessment would typically be the responsibility of other stakeholders, however ITCAs should maintain awareness of these other approaches as they relate to their program offerings.

- **Security Architecture Review** is a form of paper and pencil exercise to discuss the configurations and security posture of a particular system, which often includes not only that system but how that system is connected to other systems and devices. This type of test can also include policy review and how it affects the organization and systems the policies govern.

- **Vulnerability Assessments is** a form of assessment that uses tools to find known vulnerabilities in systems by analyzing the system version, retrieving its configuration, and comparing them to the vulnerability databases leveraged by the tools. Utility security departments or a contracted specialized security firm they hire usually perform this type of assessment.

- **Penetration Testing** is a specialized form of assessment where the testing team takes on the role of the attacker and tries to find and exploit vulnerabilities in systems and devices. Testers use the same methodology that attackers often use to identify vulnerabilities in the system. Once a vulnerability is found, the testers attempt to exploit the flaw to gain a foothold in the system and begin the process again to discover additional, lower level vulnerabilities that weren't previously exposed. Penetration testing is distinguished from vulnerability assessments by the fact it tests the depth of vulnerabilities instead of simply breadth, focus on discovering both known and unknown vulnerabilities, and provide the testing team with a better understanding of a vulnerability's risk to the business.

- **Security Code Review** is a form of assessment performed to identify security flaws in the source code of systems and devices. Vendors usually perform this type of assessment since system source code is not usually provided to the customer. However, in some instances a vendor may provide the source code to a third-party assessment laboratory, if a non-disclosure agreement is in place.

- **Compliance Review** is a form of assessment that focuses on the existence and execution of security policy. This can be performed to fulfill a formal regulatory requirement such as

NERC CIP or an informal, internal assessment to determine compliance with such guidance documents as the NISTIR 7628, security profiles from the Advanced Security Acceleration Project (ASAP-SG), or other non-regulatory documents.

- **Verification and Validation (V&V) Testing** or **Final Acceptance Testing (FAT)** is a final step of an electric utilities' purchasing and deployment process, to confirm that the system meets business requirements and fulfills its intended purpose. This type of assessment can include one or more of the assessments listed above, including penetration testing.

Each cybersecurity testing laboratory should follow a documented cybersecurity testing framework or methodology to perform all of their cybersecurity testing. Some of the most common cybersecurity testing frameworks are:

- **The Common Criteria for Information Technology Security Evaluation (Common Criteria or CC)** is an international standard (ISO/IEC 15408) for computer security certification. Common Criteria is a framework in which computer system users can specify their security functional and assurance requirements, vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims. http://www.commoncriteriaportal.org/.

- **The Information Systems Security Assessment Framework (ISSAF)** testing methodology is designed to evaluate network, system and application controls. http://www.oissg.org/issaf

- **NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*** is written to facilitate security control assessments conducted within an effective risk management framework. Special Publication 800-53A is a companion guideline to Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*.

http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf.

- **The Open Source Security Testing Methodology Manual (OSSTMM)** provides a scientific methodology for the accurate characterization of operational security (OpSec) through examination and correlation of test results in a consistent and reliable way. This manual is adaptable to almost any audit type, including penetration tests, ethical hacking, security testing, vulnerability testing, red-teaming, blue-teaming, and so forth. It is written as a security research document and is designed for factual security verification and presentation of metrics on a professional level.
  http://www.isecom.org/mirror/OSSTMM.3.pdf

- **The Penetration Testing Execution Standard (PTES)** is a standard designed to provide both businesses and security service providers with a common language and scope for performing penetration testing. The standard defines a baseline for the minimum effort required for a basic pentest, and includes several higher "levels" to provide more comprehensive activities for organizations with higher security needs.
  http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

- **NIST SP800-115, *Technical Guide to Information Security Testing and Assessment*** is a guide to the basic technical aspects of conducting information security assessments. It presents technical testing and examination methods and techniques that an organization might use as part of an assessment, and offers insights to assessors on their execution and the potential impact they may have on systems and networks.
  http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.

- **NIST SP800-142, *Practical Combinatorial Testing*** is a method that can reduce cost and increase the effectiveness of software testing for many applications by testing combinations of parameters that provides highly effective fault detection.
  http://csrc.nist.gov/groups/SNS/acts/documents/SP800-142-101006.pdf.

6.5. Additional Cybersecurity Testing Laboratory Best Practices to Consider

Along with the cybersecurity testing concepts, environments, and framework considerations described above, the following provides additional cybersecurity testing best practices for a cybersecurity testing laboratory to consider:

- The cybersecurity test team members should subscribe to a specific code of ethics. An organization like the National Board of Information Security Examiners (NBISE), https://www.nbise.org, helps to validate hands-on skills and knowledge in order to reliably predict an individual's future performance and aptitude for cybersecurity.
- A risk and threat analysis should be provided for the item to be tested. A risk and threat analysis provides information to the test team about actions that may be harmful to an implementation and the sources of the actions. In order to understand the security of the implementation being tested, both the threats an implementation is expected to address as well as the threats that are not addressed need to be known. Particularly threats that are intended to be addressed by mitigations external to the implementation need to be documented to properly scope and bound the test to be performed.
- Existing cybersecurity test programs should be leveraged when possible. Integrating existing cybersecurity test programs into a cybersecurity testing program allows for the expertise and experience from other cybersecurity testing domains to be applied. However, understanding the limits of existing cybersecurity testing programs is required in order to integrate those programs appropriately. By leveraging existing cybersecurity testing programs, it may reduce the time and cost of the testing process.
- Component cybersecurity testing should be included in cybersecurity test programs when possible. When a software or firmware component contains vulnerabilities and is reused throughout a product line, those vulnerabilities could be within multiple products. Testing at the component level ensures that the layered cybersecurity within a product continues to

protect the information and processing. Components often require re-interoperability testing when used in a different configuration to ensure proper setup and use.

- Cybersecurity testing programs should ensure they align with the business and technical requirements for the enterprise, unit, product, etc. When cybersecurity testing programs align with business, system, and technical requirements, risk can be limited and the product will have cybersecurity designed into the components and systems, so it can be part of the core testing and not an add-on "feature" to be tested.

6.6. Role of the Cybersecurity Testing Providers

Cybersecurity testing is typically conducted by information system developers, system integrators, certification agents, information system owners, auditors, inspectors general, and the information security staffs. Cybersecurity testing services, whether provided by an element within the customer's organization or a contracted public or private sector entity should demonstrate a variety of different capabilities. The cybersecurity testing provider should have a management structure that provides the framework for testing teams to conduct effective cybersecurity testing. The cybersecurity testing provider should be able to perform administrative functions to support the testing teams, protect the information received from the customer, and develop and implement standard procedures to ensure that all testing teams provide consistent, reliable and repeatable testing services. Cybersecurity testing providers assemble appropriate individuals to make up a testing team. The team members that work together to prepare for, conduct, and document the findings of the testing. Each team is made up of individuals that should collectively have the knowledge, skills, and abilities to conduct the cybersecurity testing.

Organizational management capability for a cybersecurity testing provider is the implementation of a management system that sufficiently enables a service provider to manage, plan, conduct, and assure quality of cybersecurity testing services. The cybersecurity testing provider should have an operational and management system in place in order to effectively manage and conduct cybersecurity testing. The management system framework should include: (i) maintaining independence to

prevent a conflict of interest when conducting the cybersecurity testing; (ii) implementing an effective management structure that provides both technical oversight and administrative support; (iii) providing the resources to select an effective testing team with the knowledge, skills, and abilities to conduct the testing based on the customer's product's cybersecurity claims; (iv) protecting customer information collected during the cybersecurity testing process; and (v) implementing or creating tools, templates, and standard cybersecurity testing procedures to ensure each testing team provides consistent service. Customers should be confident that the cybersecurity testing provider's cybersecurity testing teams have the knowledge, experience, and resources to conduct an effective cybersecurity test.

6.7. Cyber Security

The Cyber Security section outlines the requirements which SHALL be used by the ITCA to validate the security-related components of the interoperability testing program.

Sec-x	Cyber Security Improvements Process
	Requirements Description
Sec-1	The ITCA SHALL define the procedures and processes which will be used to validate interoperability cyber security requirements.
Sec-2	The testing and certification program SHALL ensure that defined cyber security functional performance requirements are evaluated with specific test cases in the TSS.
Sec-3	Where applicable, the ITCA SHALL have a process in place to select and implement a Digital Certificate Issuance mechanism that may include the election of a Certificate Authority. The energy ser-

	vice providers can use this certificate for authentication that a given product has actually been certified.[11]
Sec-4	The ITCA SHALL be responsible for certificate management including issuance, maintenance and policing. The ITCA can choose to outsource this responsibility as long as they remain responsible for the interoperable outcome.
Sec-5	The ITCA SHALL implement a process to qualify testing personnel at an appropriate level for their cyber security test training and experience.
Sec-6	The ITCA SHALL specifically require a test methodology that includes widely-accepted stress testing processes including static analysis and penetration testing.
Sec-7	The ITCA SHALL assure that cyber security models are policy driven, and testing SHALL also be based on policy settings.
Sec-8	The ITCA SHALL ensure that processes are in place for vendors to submit threat analysis as part of the certification process.
Sec-9	ITCA SHALL document existing security programs and standards which have been used to develop specific security testing.
Sec-10	The ITCA SHALL ensure that processes are in place to incorporate component-based cyber security concepts in the testing program.
Sec-11	The ITCA SHALL ensure that the testing laboratories have and maintain hardware, software, other equipment and facilities necessary for performing specified cyber security tests.

878

[11] Optional for ITCAs that result in interfaces and not result a physical product.

879

880

881

7. Interoperability Certification Body and Test Laboratory Requirements

The ITCA SHALL provide oversight and program requirements enforcement for the Interoperability Testing Laboratories and Certification Bodies in its programs responsible for the implementation of testing and certification activities associated with specified standards. The ITCA is also expected to cooperate with relevant SSOs and user groups for continuous improvement of the program and the standard being addressed.

Certification Bodies and Test Laboratories are required to be third party accredited to ISO/IEC Guide 65 and ISO/IEC 17025 respectively. These accreditations are attained through assessment by independent accrediting organizations. This section of the IPRM provides additional and supplemental requirements for the use of independent accreditors in assuring that ITCA program specifications for their certification bodies and test labs are clearly defined and communicated, and for use in assessing these organizations for their role supporting ITCAs.

7.1. Requirements for Certification Bodies and Test Laboratories

The requirements are comprised of three major categories which will be required by the ITCA to effectively manage the testing and certification functions of their organization.

Note: Many of the below items are more formally defined in the ISO 65 and 17025 standards.

The three major categories are:

- Governance
- Lab Qualification

- Improvement

The IPRM requirements are written with the key word "SHALL". However, depending on the ITCA program and relevant standard under consideration, some requirements may not be applicable for all situations.

.

7.2. Governance

Governance defines the structures, policies, rules and regulations associated with the ITCA certification program. The following list of Interoperability Governance Process Requirements provided in Table 1 SHALL be considered governance process requirements for managing the interoperability testing and certification programs.

Govern-x	Interoperability Governance Process
	Requirement Description
Gov-1	An ITCA Certification Program SHALL clearly identify the Standard(s) to which testing or certifications are assessed. The ITCA SHALL provide oversight to provide confidence that implementations of Standard(s) in certified products are indeed interoperable.
Gov-2	If an ITCA permits first party testing, the-ITCA SHALL clearly define the circumstances under which such testing may be submitted to a certification body and the duties of the certification body in determining the suitability of first party test data.

Gov-3	If an ITCA requires third party testing, the ITCA SHALL clearly identify the circumstances under which such testing SHALL be submitted to a certification body and the duties of the certification body in reviewing the third party test data.
Gov-4	The ITCA SHALL define a corrective process for resolving reported interoperability problems (e.g. in the field or as part of the test) for products for which they are responsible.[12] Further, it SHALL implement preventative processes to avoid recurrence of such problems. A problem may be associated with the specification, the test processes and procedures or the test data.
Gov-5	The ITCA SHALL define roles, responsibilities, and resource elements of the interoperability program in documented Certification Program requirements..
Gov-6	The ITCA SHALL specify method(s) for reporting issues to appropriate parties for resolving certification difficulties (vague or inconsistent specifications or test methods, incompatibility with similarly certified products, etc.).
Gov-7	The ITCA SHALL maintain a certified product and systems list. This list SHALL be publicly available.
Gov-8	The ITCA SHALL maintain a test case reference and modification history list.[13]
Gov-9	Test Suite Specifications (TSS)[14] used for interoperability or conformance testing SHALL be managed in a well-defined, open and formal manner with change control.

[12] The ITCA should use best efforts in contacting a standards body with respect to a specification; however, it is not their responsibility to resolve issues with the specification.
[13] See Glossary of Terms for definition and explanation of the test case reference list.
[14] See Glossary of Terms for definition and explanation of the TSS.

Gov-10	A common TSS SHALL be established when multiple test labs are deployed to test the same standard and / or profile. If common unique test procedures are required to support this test suite, then they SHALL also be defined. The TSS should be test tool agnostic.
Gov-11	All certification bodies operating under the ITCA Certification Program SHALL be accredited as meeting ISO/IEC Guide 65. The accreditation scope SHALL include the International Classification for Standards (ICS) Codes applicable to the technologies for which certification activities are performed. Accreditation SHALL be by an accreditation body that is signatory, in good standing, to the International Accreditation Forum (IAF) multilateral agreement for "Product."
Gov-12	If an ITCA has multiple testing laboratories and certifying bodies, processes SHALL be in place to avoid quality differences and assure repeatable testing between the laboratories.
Gov-13	The ITCA SHALL ensure that the test labs and certification bodies maintain their accreditation for participation in the Certification Program.-

Table 1 – Interoperability Process Governance Requirements

7.3. Lab Qualification

Lab qualification defines the requirements in Table 2 that SHALL be applied by ITCAs when recognizing testing laboratories. It should be noted that additional requirements are further detailed in ISO 17025.

Lab-x	Interoperability Lab Qualification Process
	Requirement Description
Lab-1	In selecting test organizations, the ITCA SHALL have uniform and transparent procedures for evaluating test labs.
Lab-2	The ITCA SHALL define requirements to qualify the personnel involved in the certification and testing processes.
Lab-3	The ITCA SHALL require that its test labs be accredited to ISO 17025. The accreditation scope SHALL include the specific standards or specifications against which testing may be performed. Accreditation SHALL be by an accreditation body that is (a) a signatory, in good standing, to the International Laboratory Accreditation Cooperation (ILAC) mutual recognition arrangement; or (b) recognized under the (US) National Cooperation for Laboratory Accreditation (NACLA).

Table 2 – Interoperability Lab Qualification Process Requirements

940 ## 7.4. Improvements

941 The Improvements section outlines the controls that will need to be in place to support the
942 interoperability testing processes.

943

Improv-x	Interoperability Improvements Process
	Requirements Description
Improv-1	The ITCA SHALL implement monitoring and auditing programs to ensure adherence to its policies. This is in the ISO 65 document.
Improv-2	The ITCA SHALL establish a checklist for the auditing of the appointed evaluation laboratories.
Improv-3	The ITCA SHALL periodically audit the laboratories at appropriate intervals to ensure laboratories uphold necessary capabilities.
Improv-4	The ITCA SHALL establish an auditing procedure and implement audits to verify that product interoperability is maintained after the product passes the testing and certification programs and enters the market.
Improv-5	The ITCA SHALL have processes in place, including corrective and preventative actions, which results in continual improvement of their testing and certification programs.
Improv-6	The ITCA SHALL be in constant communication with the standards writing committees to create a feedback loop. For example, the ITCA should define a process to communicate the TSS test results back to the SSOs and stakeholders.
Improv-7	The ITCA SHALL provide a forum for feedback to be received from a stakeholder, interested business party and use case in order to improve its interoperability best practices.

Improv-8	It is preferred that ITCAs have a method for actively soliciting interoperability feedback on implementations of the standard in order to achieve some level of customer and user-community satisfaction on that feedback.

944 **Table 4 – Interoperability Improvements Process Requirements**

945

8. References

NIST Framework and Roadmap for Smart Grid Interoperability Standards

ISO 17000 - Conformity Assessment - Vocabulary and general principles

ISO 17011 - Conformity Assessment - General requirements for accreditation bodies accrediting conformity assessment bodies

ISO 17025 - General requirements for the competence of testing and calibration laboratories

ISO Guide 65 - General requirements for bodies operating product certification systems

ISO Guide 67 - Conformity assessment - Fundamentals of product certification

9. Glossary of Terms

Accrediting Body – Organization that formally evaluates processes of test laboratories or certification bodies with respect to specific standard(s) or specification(s).

Application Profile - A selected subset of the product and / or standard which can be used to implement a particular feature set or use case scenario.

Attestation - Issuance of a statement that fulfillment of specified requirements has been demonstrated.

Certificate – Unique identifier of a particular product. It applies to both software and hardware products. The certificate can be a physical or digital artifact (e.g., X.509 PKI schemes require digital certificates).

Certification – Third-party attestation related to products, processes, systems or persons.

Certification Bodies (CBs) – The entity responsible for certifying that products have fulfilled the requirements of a standard or specification.

Compliant Portion Description (CPD) – A CPD is a definitive manifest of all mandatory and optional features implemented in a certified product. The CPD is generally used by product designers to judge:

- Conformance of an implementation,
- Completeness of a system composed of pre-certified sub-components by comparing each of the CPDs of those sub-components.
- Interoperability of two products based on matching feature sets as described by their respective CPDs.

For example, a designer can compare the CPD with the test requirements to determine the level of conformance of a product to a specification. When designing a product composed of pre-certified sub-components, the respective CPDs will serve as selection criteria to design the complete product. The CPD also helps to judge the level of interoperability that can be expected from interactions between two independent implementations. A client service and a server function can be reviewed for their expected level of interoperability solely based on their respective CPDs.

Conformance Certification – A third-party attestation that a product conforms to a standard or specification.

Conformance Testing – Determines whether an implementation conforms to the standard as written. This is done by evaluating the implementation with a test tool such as an emulator, test harness, golden unit, etc.

Feature set – A feature set is a particular characteristic of a product based on a particular use case scenario. For example: signaling price is a feature set.

First Party Testing – is when an implementer self-tests their own product. This is usually permitted after a technology has matured to where sufficient tools and specifications enabling first party testing are available to all vendors.

Golden Implementation/Units – Test tools that can be configured in a laboratory to provide a constant baseline or reference such that there is assurance that changes to the products making up a system under test or configuration variants are consistently tested in the same manner

Inheritance – Those actions required to evaluate the compatibility of a proposed inherited design including products, subsystem functions and design requirements.

Interoperability – Ability of a product or system to work with or integrate with another product or system based on defined business requirements.

Interoperability Testing – Connects two or more implementations together and determines whether they can successfully communicate. Significantly different from conformance testing, it is often possible for two systems that conform to the standard to be unable to communicate. If they can communicate, it is possible that they cannot perform any useful functions. These situations arise because the implementations have conflicting interpretations of the specification, or because they have chosen conflicting options within the standard. A particular form of interoperability testing is application testing, in which there is a specification for the particular use of standard that can be tested.

Implementation Under Test (IUT) – The implementation subject to testing. Covers System Under Test (SUT) and Device Under Test (DUT)

Multi-vendor and Multi-product Testing Event – An interoperability test of products with other peer products. The outcome of the testing is used to improve both products and the specification.

Performance / Protocol / Proforma Implementation Conformance Statement (PICS) – Defines all mandatory and optional feature sets of a specification that can be used to implement a product.

Platform level communications protocol - In the IPRM, platform level communications protocols are integrated products based on standards only associated with layers 1 and 2 of the OSI layer. (e.g., Wi-Fi platform)

Second Party Testing – Testing activities performed by buyers and users.

Security Testing – Analyzes whether the implementation correctly makes use of any security features from the standard or other security features available in the product. This is the most difficult type of testing program since it must evaluate whether the system has vulnerabilities, which are not always obvious.

Standards Setting Organizations (SSOs) - An association whose primary activities are developing, coordinating, promulgating, revising, amending, re-issuing, interpreting, or otherwise maintaining standards. A Standards Developing Organization is one form of a Standards Setting Organization. Example SSOs including International Organization for Standardization (ISO), International Electro technical Commission (IEC), Institute of Electrical and Electronics Engineers (IEEE), American National Standards Institute (ANSI), etc. An SSO can also be an industry trade association that develops industry standards such as the ZigBee Alliance.

Static Conformance Review – A review of designed feature sets versus the specified PICS to determine the extent to which the features are supported by the IUT. This is the first step when a product enters a testing program. Generally the test lab requests that the implementer declare all supported feature sets in a product. This information is used to create the test plan for that product.

Test Cases – A set of tests to verify a particular feature set. There are many ways to test a feature set, with each of those representing a test case. Generally, a program defines all possible test cases in the test specification document.

Test Case Reference List – A current master list of all tests that are to be included into a product test plan. This list also indicates the time variable applicability of each test by reflecting those tests

which are no longer valid, and those that are not currently valid but are scheduled to become active in the near future. This helps a product implementer in preparing fully conforming and interoperable products for an upcoming launch.

Test Harness - Collection of software, test data, and hardware configured to test a product by operating it under varying conditions and monitoring its behavior and output.

Test Interface - The programmatic application interface to enable communication between a test harness and system or device under test.

Test Plan – A Test Plan is a list of applicable tests for a specific product and is derived from the Test Case Reference List.

Test Procedure – A stepwise test method of a particular test case. An example of a test procedure can be the steps needed for an Energy Services Interface (ESI) to send price signals, which may include configuring the time information, updating price tables, etc.

Test Profile or Profile - A select subset of a product and / or standard to implement a particular test of a feature or a use-case test. Test Profiles evaluate a subset of a TSS and are used to target specific areas of product interoperability.

Test Resource - Any information, equipment, material, and support required to implement testing.

Testing – According to EN 45020, testing is defined as “the technical operation that consists of the determination of one or more characteristics of a given product, process or service according to a specified procedure”.

Testing Laboratories (TLs) – Test service providers for a standard or specification.

Test Suite Specification (TSS) or Test Spec- Consists of a suite of tests, categorized into logical functional areas, such as use cases or well-defined features. Each test suite consists of many related test cases corresponding to a particular feature set or use case. Test cases would include both valid and invalid behavior tests. Each test case is further described step-by-step with test procedures and well defined pass / fail / indeterminate criteria, along with references.

Test Suite- A collection of related test cases. A test suite can be put together to test a feature set. A pricing test case would be in a "price test suite" but a messaging test case would be in a "messaging test suite".

Third Party Testing – Testing activities performed by organizations independent of first or second parties.

Use Case - A description of a system's behavior as it responds to a request that originates from outside of that system

INFORMATIONAL ANNEXES

A. Working Group

Interoperability Process Reference Manual (IPRM) – Working Group #4	
Leadership	
Rik Drummond, Chair	
Rolf Bienert, Co-Chair	
Rudi Schubert, Project Manager	
IPRM Version 2 Editing Team Members	
Rik Drummond	Drummond Group
Rudi Schubert	Enernex
Dean Prochaska	NIST
Marianne Swanson	NIST
Don Heirman	Heirman Consultants
Sandy Bacik	Enernex
Kent Donohue	Underwriters Laboratories
Rolf Bienert	TUV Rheinland
James Mater	Quality Logic
Zahra Makoui	PG&E
Donny Helm	Oncor
Tobin Richardson	Zigbee Alliance
John Adams	Honeywell
David Alderman	NIST
Phil Beecher	Beecher Communications Consultants
Peter Cain	Agilent
Kent Dickson	Tendril
Lawrence Durante	National Grid
Greg Ennis	WiFi Alliance
Margaret Goodrich	SISCO
Chris Held	GE Energy
Mladen Kezunovic	Texas A&M
Lanse LaVoy	DTE Energy
Gary McNaughton	Cornice Engineering
Ian Mundell	PJM Interconnection
Bruce Muschlitz	EnerNex
Emily O'Brien	KEMA
Mark Ortiz	Xtensible Solutions

Interoperability Process Reference Manual (IPRM)

Clint Powell	Powell Wireless Commsulting
John Simmins	EPRI
Ravi Subramaniam	IEEE-ISTO
Tim Worthington	GE Energy
Tony Youssef	Cisco Systems
Listserv Information	
To send an e-mail to the IPRM working group list: SGIP-SGTCC-IPRM@SMARTGRIDLISTSERV.ORG To subscribe to the IPRM working group, go to the following address: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGridTestingAndCertificationCommittee select **Join SGIP-SGCTCC-IPRM listserv**.	

1083

B. Document History

Revision Number	Revision Date	Revision By	Summary of Changes
1	8/30/11	Rudi Schubert	First outline of IPRM V2 prepared for IPRM working group review and comment
2	10/22/11	Rudi Schubert	IPRM V2 – Official 1st draft for SGTCC comment released
3	11/3/11	Rudi Schubert	IPRM V2 – Official 2nd draft for SGTCC comment released; incorporates most comment received on prior draft, with additional comments tabled for further working group discussion
4	11/23/11	Rudi Schubert	IPRM V2 – Official 3rd draft for SGTCC comment released; incorporates most comments received on prior draft and some re-organization of content from prior version
5	12/15/11	Rudi Schubert	IPRM V2 – Final Draft – incorporates comments and resolutions that were discussed and agreed upon during the SGTCC 2011 winter meetings